 <p>County of Kaua'i</p>	<p>Procedures for Protecting Personal Information</p>	<p>Documentation Number: ITP0030</p> <hr/> <p>Revision Level: 4/21/09</p>
--	--	---

I. SCOPE / PURPOSE: The purpose of this policy is to describe the County of Kauai's (COK) procedures for protecting documents containing Personal Information.

Background:

The 2008 Hawai'i Session Laws Act 10 was enacted on July 8, 2008. The purpose of Act 10 is to implement recommendations of the Hawai'i Identity Theft Task Force's December 2007 report to protect the security of personal information collected and maintained by state and county government agencies.

II. RESPONSIBILITY: All County of Kauai agencies, boards and commission are responsible for safeguarding the confidential information with which we have been entrusted in serving the citizens of Kaua'i. Identity theft is one of the fastest-growing crimes in our state, and the proper handling of any personal information within our control is a paramount concern to the County of Kaua'i. This responsibility requires the continuing diligence of all of our employees to limit the potential for mishandling or losing personal information. Accordingly, the following procedures are to be implemented immediately and must be observed by all employees.

III. DEFINITIONS:

"Personal Information" is the First Name or First Initial, and Last Name, in combination with any one of the following:

- Social Security Number
- Driver's License Number or Hawai'i ID Number
- Account Number, Credit or Debit Card Number, Access Code, or Password that would permit access to an individual's financial account.


IV. PROCEDURE:

A. Document Storage

The following procedures must be observed for storing confidential documents:

1. All hardcopy confidential documents maintained by the agency shall be stored in a secured area accessible to only those employees whose job function requires them to handle such documents. A secured area includes a locked drawer, cabinet, or room. Access to these areas must be controlled and monitored.

Prepared by: Nyree Norman	Date last revised: 4/21/09	Page Number: 1/6
Original release date: 12/24/2008	Reviewed by : Eric Knutzen Approved by: Wallace Rezentes	

 <p>County of Kaua'i</p>	<p>Procedures for Protecting Personal Information</p>	<p>Documentation Number: ITP0030</p>
		<p>Revision Level: 4/21/09</p>

2. All electronic confidential documents maintained by the agency shall be safeguarded against possible misuse by complying with the Information Technology Computer Use, USB Flash Drive, Standard Mobile Device and Document Destruction Policies as attached in Exhibit A, B, C, and D respectively.

B. Document Processing

Business needs frequently require that confidential documents be removed from secured areas in order to perform necessary job functions. The following procedures shall be followed when such documents are in possession of an employee in the course of the employee's job duty.


1. When not in a secured area, the confidential documents must not leave the employee's immediate control. Documents of this nature cannot be left unsupervised while physical controls are not in place.
2. When not in a secured area, precautions must be taken to obscure the confidential information from view, such as by means of an opaque file folder or envelope. Confidential information shall not be left in plain view in a vehicle.
3. Confidential documents must be inspected thoroughly to ensure they do not contain any misfiled confidential information from other files.
4. To protect electronic confidential documents, all employees shall leave their computers in a 'locked or 'logged off' state, when not in immediate vicinity of the employee's work area.
5. The County shall strive to redact personal information in electronic documents where possible, reduce any unnecessary collection of personal information, and ensure data is properly encrypted on all mobile devices.

C. Document Shipping

Shipping to an Individual or Business

Business functions frequently require that personal information be mailed to external destinations, such as Contracts, RFPs, etc. When in transit, these


<p>Prepared by: Nyree Norman</p>	<p>Date last revised: 4/21/09</p>	<p>Page Number: 2/6</p>
<p>Original release date: 12/24/2008</p>	<p>Reviewed by : Eric Knutzen Approved by: Wallace Rezentes</p>	

 <p>County of Kaua'i</p>	<p>Procedures for Protecting Personal Information</p>	<p>Documentation Number: ITP0030</p> <hr/> <p>Revision Level: 4/21/09</p>
--	--	---

materials are not in our immediate control and must be secured to the best of our ability beforehand. The following procedures must be observed when shipping confidential documents:

1. Preparation of Documents
 - a. Documents must be packaged in such a way as to not have any personal information viewable.
 - b. All destination addresses must be inspected thoroughly and confirmed to avoid delivery to a wrong address or person.
 - c. Ensure that the correct return address is provided in the event the package is undeliverable.
 - d. Contents of shipments must be verified to contain only appropriate information for the intended recipient.
2. Shipping Materials
 - a. Use shipping envelopes made of fibrous or polymeric material or reinforced shipping boxes made of sturdy corrugated material with a limited number of seams.
 - b. Ensure the container is the appropriate size to accommodate the secure and safe delivery of contents.
 - c. Storage containers, including certain archive boxes, are not considered suitable for shipping as they are collapsible and damage easily when navigating large distribution center equipment and processes.
 - d. Never reuse shipping containers that are worn or have been torn. Use super strength, 2 inch wide packaging tape.
 - e. Secure all seams of package with tape. Run tape completely around package, not just the flap and bottom seam. Secure package further by running tape horizontally and vertically around the center of the package.
3. Package Labeling
 - a. Be sure the shipping label includes a complete recipient name, address, and, for businesses, telephone number; and, that it also includes the sender name, return address and telephone number. The telephone numbers provide a means of contact when/if for some reason the package is misrouted or damaged during the shipping process.
 - b. Make sure the entire label is securely affixed to the center front of package and it is clearly visible.
 - c. DO NOT MARK THE PACKAGE CONFIDENTIAL.

<p>Prepared by: Nyree Norman</p>	<p>Date last revised: 4/21/09</p>	<p>Page Number: 3/6</p>
<p>Original release date: 12/24/2008</p>	<p>Reviewed by : Eric Knutzen</p> <p>Approved by: Wallace Rezentes</p>	

 <p>County of Kaua'i</p>	<p>Procedures for Protecting Personal Information</p>	<p>Documentation Number: ITP0030</p>
		<p>Revision Level: 4/21/09</p>

4. Shipping Method
 - a. Packages containing confidential material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

D. Shipping between Offices

All files and records being shipped between County offices or between County and external associates must employ all of the above procedures and the following:


1. Inventory of Confidential Documents
 - a. Shipper is to inventory and document all records being shipped prior to shipping.
 - b. The inventory record includes, at a minimum, the name and tracking number of the record(s) being shipped, the destination, the sender name and contact number, the recipient name, the date shipped and a place to record the date of when the shipment reaches its destination.
 - c. An electronic copy of this inventory must be emailed to the intended recipient notifying them of the pending arrival.
2. Timely Acknowledgment
 - a. Shipper is to include a copy of the inventory document in the shipping container so that the recipient can verify contents of shipment upon arrival and acknowledge to sender that all record(s) were received.
 - b. If a shipment has not been acknowledged by a recipient within 24 hours, shipper will follow-up with the recipient office and/or shipping organization as appropriate.

E. Breach Notification and Incident Reporting

If documents containing confidential information are improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. An employee shall notify the Information Technology Help Desk Administrator, and an incident-report (Exhibit D as attached) form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.

<p>Prepared by: Nyree Norman</p>	<p>Date last revised: 4/21/09</p>	<p>Page Number: 4/6</p>
<p>Original release date: 12/24/2008</p>	<p>Reviewed by : Eric Knutzen Approved by: Wallace Rezentes</p>	

 <p>County of Kaua'i</p>	<p>Procedures for Protecting Personal Information</p>	<p>Documentation Number: ITP0030</p>
		<p>Revision Level: 4/21/09</p>

2. The supervisor will communicate the situation to the reception staff or those that regularly field calls from the public so that they are prepared to answer phone inquiries by individuals who have been notified of the loss or disclosure of their records.
- F. Each agency, board and commission is responsible to inform the Mayor's ISPC appointee of any additional use of personal information or pertinent changes to forms.
- G. The County agencies, boards and commissions are advised not to do any of the following:
1. Intentionally communicate or otherwise make available to the general public entire SS#.
 2. Intentionally print or imbed entire SS# on any card required to access products or services.
 3. Require entire SS# to access an Internet website, unless a password or unique personal identification # or other authentication device is also required to access the website.
 4. Print entire SS# on any material that is mailed, unless the materials are employer-to-employee communications or where specifically requested by the individual.


H. Consequences

It is the responsibility of agency supervisors to ensure their staff's compliance with these procedures. Failure by the agency employees to comply with the procedures defined in this directive may result in disciplinary action.

I. Authority

**CHAPTER 487N
SECURITY BREACH OF PERSONAL INFORMATION**

<p>Prepared by: Nyree Norman</p>	<p>Date last revised: 4/21/09</p>	<p>Page Number: 5/6</p>
<p>Original release date: 12/24/2008</p>	<p>Reviewed by : Eric Knutzen Approved by: Wallace Rezentes</p>	

 County of Kaua'i	Procedures for Protecting Personal Information	Documentation Number: ITP0030
		Revision Level: 4/21/09

V. ATTACHMENTS:

Exhibit A - Information Technology Computer Use Policy
 Exhibit B - USB Flash Drive Policy
 Exhibit C - Standard Mobile Device Policy
 Exhibit D - Document Destruction Policy
 Exhibit E - Personal Information Security Incident Report Form

VI. ANNUAL REVIEW, REPORTING, POLICY AND OVERSIGHT RESPONSIBILITY

The Mayor's appointee to the statewide Information, Security and Privacy Council (ISPC) is responsible to conduct an annual review of this policy, as well as to have county oversight regarding the protection of personal information. The County will work with identification of collection of unnecessary information and perform an annual review regarding the potential of any unnecessary collection of personal information, as well as redaction personal information. Furthermore, an annual report is to be submitted to the County Administration as well as to the ISPC, following any timeline so published by the ISPC.

VII. REFERENCES

For a copy of this policy or any documents referred to within this policy please refer to the following Personal Information Document Library link:

<http://cok-sp-01/Personal%20Information%20Document%20Library/Forms/AllItems.aspx>

Prepared by: Nyree Norman	Date last revised: 4/21/09	Page Number: 6/6
Original release date: 12/24/2008	Reviewed by : Eric Knutzen Approved by: Wallace Rezentes	